
| Issue Date |
| --- |
| September 30, 2009 |
| Audit Report Number |
| 2009-DP-0007 |

TO: Nelson Bregón, General Deputy Assistant Secretary for Community Planning and Development, D

FROM: Hanh Do, Director, Information Systems Audit Division, GAA

SUBJECT: Review of Selected Controls within the Disaster Recovery Grant Reporting System

# HIGHLIGHTS

## What We Audited and Why

We audited selected controls within the Disaster Recovery Grant Reporting system (DRGR) related to Neighborhood Stabilization Program (NSP) funding because of the emergency and the transparency nature of the Housing and Economic Recovery Act and the American Recovery and Reinvestment Act, respectively, and corresponding statutory timeframes. DRGR is an existing system that was modified to track close to $5.9 billion dollars of NSP funds, the majority of which must be obligated and expended within two years. NSP I funding totaled $3.9 billion. The American Recovery and Reinvestment Act of 2009 (ARRA) revised some of the program rules and appropriated an additional $2 billion for the program, to be competitively awarded. Following the initiation of our audit, the Office of Community Planning and Development (CPD) decided to use DRGR to track the $2 billion in funding allocated to NSP II, in addition to the $3.9 billion allocated to NSP I. Although the U.S. Department of Housing and Urban Development (HUD) has made significant modifications to DRGR within the last 18 months, HUD did not have sufficient time to develop a new system or modify an existing system to perfectly fit NSP. We focused our review to assess risk assessment updates and whether NSP funds were properly safeguarded by the access controls related to DRGR.

## What We Found

While we did not find misappropriation or misuse of funds in our limited review, we did find weaknesses that require CPD actions to obtain reasonable assurance that NSP funds are properly safeguarded. We found that (1) access control policies and procedures for DRGR violated HUD policy, (2) the system authorization to operate was outdated and based upon inaccurate and untested documentation, (3) CPD did not adequately separate the DRGR system and security administration functions, and (4) CPD had not sufficiently tested interface transactions between DRGR and the Line of Credit Control System (LOCCS). As a result, CPD could not ensure that only authorized users had access to the application, user access was limited to only the data that were necessary for them to complete their jobs, and users who no longer required access to the data in the system had their access removed. In addition, the application had been operating under an outdated security certification for seven months. Although CPD had initiated the authorization process, it was initiated without updated accurate documentation; therefore, any results would also be based upon inaccurate information. The failure to properly assign the help desk function led to an inefficient use of staff resources and may have caused unnecessary delays to users in getting assistance. The failure to sufficiently test interface transactions between DRGR and LOCCS left HUD with limited assurance that the $5.9 billion in NSP funding was accurately processed.

CPD had identified and initiated actions in an effort to address or mitigate many of the weaknesses identified. We commend CPD's efforts to identify and remedy the weaknesses in the DRGR system. In addition, we acknowledge that CPD efforts to initiate and proceed with modifications to DRGR have been hampered due to a lack of funding and staff resources.

## What We Recommend

We recommend that CPD (1) formalize the user access request process and strengthen access controls; (2) update and correct system documentation and resubmit the revised documentation for security certification and accreditation; (3) separate the duties of system and security administration and reassign the help desk functionality; and (4) work with its contractors to ensure that tests of drawdown controls and transaction processing reports are performed as stated in the functional requirements documentation or, if other controls are used, remove from the system documentation stated controls that are not in use.

For each recommendation without a management decision, please respond and provide status reports in accordance with HUD Handbook 2000.06, REV-3. Please furnish us copies of any correspondence or directives issued because of the audit.

## Auditee's Response

We provided a draft copy of this report to the auditee on September 15, 2009, and the auditee provided its written comments on September 25, 2009. The auditee generally agreed with our report. The complete text of the auditee's response, along with our evaluation of that response, can be found in appendix A of this report.

# TABLE OF CONTENTS

# BACKGROUND AND OBJECTIVE

The Disaster Recovery Grant Reporting (DRGR) system was developed by the U.S. Department of Housing and Urban Development's (HUD) Office of Community Planning and Development (CPD) for the Disaster Recovery Community Development Block Grant (CDBG) program and other special appropriations. Data from the system are used by HUD staff to review activities funded under these programs and for required quarterly reports to Congress. The system was developed for grantees to identify activities funded under their action plans and amendments, to include budgets and performance goals for those activities. To receive funding, these grantees must prepare a citizen participation plan, publish their proposed use of the funds, and submit an action plan to HUD. Once an action plan is submitted and approved, grantees can submit quarterly reports summarizing obligation, expenditures, drawdowns, and accomplishments for all of their activities.

Public Law 110-289, July 30, 2008, the Housing and Economic Recovery Act of 2008 (HERA), was passed to provide needed housing reform and for other purposes. The Act designated HUD to distribute $3.92 billion in federal funds to states and local entities using the CDBG model. (The CDBG model is an entitlement program that distributes funds annually, by formula, to large communities and states as well as smaller communities and Indian reservations.) The HERA funds and distribution are known as the Neighborhood Stabilization Program (NSP) and are meant for the purchase and rehabilitation/development of foreclosed or abandoned homes and residential properties. This program is now referred to as NSP I. Eligible uses include: establish financing mechanisms for purchase and redevelopment of foreclosed upon homes and residential properties, purchase and rehabilitate homes and residential properties that have been abandoned or foreclosed upon, in order to sell, rent, or redevelop such homes and properties; establish land banks[1] for homes that have been foreclosed upon; demolish blighted structures; and redevelop demolished or vacant properties.

The American Recovery and Reinvestment Act of 2009 (ARRA) was passed on February 17, 2009 to provide federal funds for economic recovery from the recession. It revised some of the program rules for NSP I (HERA) and appropriated an additional $2 billion for NSP to be competitively awarded. HUD plans to use DRGR to administer the program's expansion pursuant to the American Recovery and Reinvestment Act. This program is now referred to as NSP II. The eligible uses noted for NSP I above were revised as follows: establish land banks for homes that have been foreclosed upon was modified by ARRA to read "establish and operate land banks for homes and residential properties that have been foreclosed upon." And redevelop demolished or vacant properties, ARRA added the following provision: Funding used for section 2301(c) (3) (E) of HERA shall be available only for the redevelopment of demolished or vacant properties as housing. In addition ARRA repealed a section of HERA related to reinvestment of profits.

[1] A land bank is a governmental or nongovernmental nonprofit entity established, at least in part, to assemble, temporarily manage, and dispose of vacant land for the purpose of stabilizing neighborhoods and encouraging re-use or redevelopment of urban property. Federal Register Notice 73 FR 58330

HUD stated that it used DRGR for the program because no other application and reporting system was sufficiently flexible to deal with the alternative requirements. HERA authorizes the Secretary to specify alternative requirements to any provision under Title I of the Housing and Community Development Act of 1974, as amended, (the HCD Act) except for requirements related to fair housing, nondiscrimination, labor standards, and the environment (including lead-based paint), in accordance with the terms of section 2301 of HERA and for the sole purpose of expediting the use of grant funds.[2] The emergency nature of the Housing and Economic Recovery Act and corresponding statutory timeframes did not give HUD sufficient time to develop a new system or modify an existing system to perfectly fit the program. DRGR was created to enhance local and national oversight of the Disaster Recovery CDBG program. It was initially a reporting and tracking system that helped HUD management track/review action plans and quarterly performance reports from grantees. HUD has made significant modifications to DRGR within the last 18 months. It has created an interface to allow grantee users to submit payment requests for funds through DRGR for payment from the Line of Credit Control System (LOCCS). In addition, modifications have been made to allow for the reporting of specific activities under NSP.

The objective of this review was to assess selected system controls within DRGR related to NSP funding. Our review was focused to assess risk assessment updates and whether NSP funds were properly safeguarded by the access controls related to DRGR. A risk assessment report allows managers to use it for evaluating the security of the information technology systems that they manage and for determining the potential for loss or harm to organizational operations, goals, and its stakeholders.

[2] Federal Register Notice 73 FR 58330

# RESULTS OF AUDIT

## Finding 1: Access Control Policies and Procedures for DRGR Violated HUD Policy

CPD did not follow HUD policy in the creation of the access control policies and procedures for DRGR. This condition occurred because CPD did not formalize the access request process. By not implementing strong access controls, HUD could not ensure that users have access to only the data that were necessary for them to complete their jobs. In addition, HUD could not be certain that only authorized users had access to the system and that users who no longer required access to the data in the system had their access removed.

### CPD Did Not Formalize Access Request Procedures for the DRGR Application

CPD granted all user access to the application on the basis of an e-mail request. For HUD users, this practice violated HUD's policy, HUD Handbook 2400.25, REV-2, section 5.2.2, requiring that access be requested through its Centralized HUD Account Management Process (CHAMP). This process was established to allow HUD to centralize and maintain records regarding system access granted to HUD applications. For grantee users, HUD granted access to users based on an authorization by HUD field office employees and not authorization from the grantee organization. Only the grantee organization should be responsible for the assignment of the duties and responsibilities of the grantee staff. To ensure that access levels are granted based on user duties and responsibilities, authorization must be obtained from the grantee organization. HUD Handbook 2400.25, REV-2, section 5.2.1 incorporates NIST 800-53 Control AC-1. In addition, the design of DRGR does not allow a grantee to use a single user identification code (ID), to access the data for more than one grantee. Therefore, when a grantee user requires access to the data of more than one grantee, the user must be assigned more than one user ID. However, the grantee organizations were not required to formally approve the additional user ID or level of access. The grantee organization must provide authorization for all user IDs, including each additional user ID. This condition occurred because CPD had not formalized access policies for DRGR.

The National Institute of Standards and Technology Special Publication (NIST SP) 800-53,[3] Control AC-1, requires the organization to develop, disseminate, and

[3] Recommended Security Controls for Federal Information Systems

periodically review/update (1) a formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and (2) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

HUD Handbook 2400.25, REV-2, section 5.2.2, requires that

- Program offices/system owners shall ensure that users of information systems supporting their programs have a validated requirement to access these systems.
- Program offices/system owners, in concert with the system security administrator, shall ensure that access privileges, which increase from greater than read only, be processed through HUD's account management system.
- Program offices/system owners shall ensure that users of information systems under their purview have approved access requests before granting access to the systems.

## CPD Did Not Require Users to Sign or Acknowledge Rules of Behavior Documents

CPD did not require all users to sign rules of behavior documents and acknowledge the rules of behavior before providing them access to DRGR. HUD Handbook 2400.25, REV-2, section 3.2.4, requires program offices/system owners to define and maintain additional rules of behavior documents when the Chief Information Security Officer generic rules of behavior are not sufficient. Since all DRGR users are not required to sign the generic rules of behavior, CPD is required to develop specific rules of behavior for access to this application. The rules of behavior should (1) clearly delineate user responsibilities and the expected behavior of all individuals with access to the system, (2) state the consequences of inconsistent behavior or noncompliance, and (3) be made available to every user before the user receives authorization for access to the system. Without signed acknowledgement from users indicating that they have read, understood, and agreed to abide by the rules of behavior related to the information systems and its resident information, CPD was exposed to several control risks including unauthorized or inappropriate use of DRGR data.

## CPD Did Not Implement a Formal User Recertification Process

CPD did not implement a formal user access recertification process for DRGR. Instead, it produced listings of grantee and HUD staff and sent these to the HUD field offices for review. A proper recertification process entails the initiation of communication between the system security administrator and each user's authorizing official. This communication should contain the user's name, access level, and any additional information required to provide the authorizing official sufficient detail of each user's access that the official is asked to reauthorize. The process should require the authorizing official to respond to the security administrator to indicate that the user still requires access to the application and what level of access the user requires. HUD Handbook 2400.25, REV-2, paragraph 5.2.2h, requires that program offices/system owners ensure that the user access for all users is reviewed once a year.

## CPD Initiated a Requirement to Have All Users Obtain Access to DRGR through CHAMP

In July, 2009 CPD initiated actions to formalize the user access policies for DRGR. These actions include a requirement that all HUD users obtain access to DRGR through the CHAMP process. As these action were on-going and not completed by the time OIG completed this audit, we did not assess or verify the completion of CPD's planned actions.

## Conclusion

By not implementing strong access controls, HUD could not ensure that users had access to only the data that were necessary for them to complete their jobs. In addition, HUD could not be certain that only authorized users had access to the system and that users who no longer required access to the data in the system had their access removed.

## Recommendations

We recommend that the Office of Community Planning and Development

1A. Complete establishment of policies and procedures requiring that all access-related requests for HUD employees be processed through CHAMP.

1B. Provide a listing of all HUD employees with access to the DRGR application and their access level to the Office of the Chief Information Officer, Office of Information Technology Support Services, for recording in CHAMP.

1C. Establish rules of behavior for each type of DRGR user. Implement policies and procedures requiring users to complete and sign the rules of behavior form when access is granted and annually at recertification.

1D. Establish a formal process for grantee users requesting access to the application. This process should include a requirement that an official from the applicant's organization authorize the request and the type of access required.

1E. Implement a formal user recertification process for all DRGR users.

# RESULTS OF AUDIT

## Finding 2: DRGR's Authorization to Operate Was Outdated and Based upon Inaccurate and Untested System Documentation

CPD did not maintain accurate system documentation and the DRGR application operated under an outdated security certification and authorization. This condition occurred because CPD did not require its contractor to provide updated documentation in a timely manner and did not review the documentation submitted for accuracy. By accepting inaccurate system documentation, the $3.9 billion in funding for NSP I and the $2 billion in funding for NSP II are vulnerable to security exposures.

### System Documentation Used in the Security Certification and Accreditation Process Was Based on Inaccurate Information

Inaccurate information was used to support the certification and authorization process for DRGR.[4] We found references to security controls in place in the most current system security plan[5] for DRGR that did not exist. Operational tests of errors, daily transaction totals, and out-of-balance reports of the drawdown of grant funds interface with LOCCS, also referenced within the DRGR functional requirement document (see finding 4), did not exist. We also found that the DRGR risk assessment, although updated, included a control that had not been implemented (rules of behavior documents, as noted in finding 1.)

According to NIST SP 800-37,[6] it is essential that agency officials have the most complete, accurate, and trustworthy information possible on the security status of their information systems to make timely, credible, risk-based decisions on

[4] Certification - A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Accreditation - The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
[5] System Security Plan - Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
[6] Guide for the Security Certification and Accreditation of Federal Information Systems

whether to authorize operation of those systems. The information and supporting evidence needed for security accreditation is developed during a detailed security review of an information system, typically referred to as security certification. The publication further states that the security accreditation package should contain an (1) approved system security plan, (2) security assessment report, and (3) plan of action and milestones. The system security plan contains an overview of the security requirements, the agreed-upon security controls, and supporting security-related documents such as a risk assessment. The security assessment report contains the security assessment results and recommended corrective actions. The plan of action and milestones contains measures, implemented or planned, to correct deficiencies and to reduce or eliminate known vulnerabilities.

## DRGR System Contingency Plans Had Not Been Tested and Neither Configuration Management nor Contingency Planning Documents Had Been Updated

The contingency plan for the DRGR application had not been tested.[7] DRGR is defined as a 'major application' and its risk impact level is categorized as moderate.[8] HUD Handbook 2400.25, REV-2, section 4.3.4, requires that program offices/system owners ensure that contingency plans for moderate- and high-impact systems are tested at least annually in compliance with the HUD contingency planning guidance and NIST SP 800-34. Testing should be coordinated with elements responsible for continuity of operations plan (COOP), critical infrastructure protection (CIP), and incident response.[9] Without testing, HUD has no assurance that plans or policies are effective.

The configuration management[10] and contingency planning[11] documents for DRGR had not been updated since they were created in 2004 and 2005. Both documents referred to contractors and HUD staff members no longer associated with the project. In addition, major modifications had been made to the

[7] Executing contingency plans during controlled tests and/or exercises provides a mechanism to test the effectiveness of the contingency plans, the training provided and correct weaknesses in the plan in a controlled situation.
[8] CPD's System Security plan defined DRGR as a major application and the Risk Assessment categorized the risk impact level as moderate.
[9] Incident - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
[10] The configuration management plan documents the policies, procedures, and guidance needed to identify, manage, and track the hardware, software, documentation, and data items generated or maintained during continued DRGR operation.
[11] The contingency plan establishes procedures to recover the DRGR following a disruption.

application, including the addition of a funds drawdown module and a large increase in the number of users, which also should have triggered an update to the plans. HUD Handbook 2400.24, REV-2, section 4.4.3, requires that program offices/system owners prepare configuration management plans and establish, implement, and enforce change management and configuration management controls for all information systems and networks under their purview. The security impact of any proposed change must be analyzed and considered during the change management process. Changes to the information system must be documented, and they must include emergency change procedures. The handbook also requires, in section 4.3.5, that program offices/system owners review contingency plans once a year, update them, and communicate any changes to the program office responsible for the COOP and CIP, if applicable, in compliance with the HUD contingency planning guidance and NIST SP 800-34.[12] Failure to update these documents implies limited tracking of system modifications since documentation is not maintained and updated.

**DRGR System Documentation Was Not Created or Updated in a Timely Manner and in Some Cases, Contained Inaccuracies**

CPD did not have system or user manuals for DRGR. This condition occurred because CPD staff responsible for the creation of the application instructed their contractor to create a system without system or user manuals. The inaccuracies were the controls stated as implemented in the documentation, but not in place during operation, as noted above. HUD Handbook 2400.25, REV-2, section 3.3.5, requires that program offices/system owners ensure that adequate documentation for the information system is available, current, protected when required in compliance with NIST guidance, and distributed to authorized personnel. The handbook specifically identifies the following as required: application documentation for in-house applications; system build and configuration documentation, which includes optimization of system security settings, when applicable; certification and accreditation and system development life cycle documentation[13]; user manuals; and configuration guidance.

[12] Contingency Planning Guide for Information Technology Systems

[13] The system development life cycle starts with the initiation of the system planning process, and continues through system acquisition and development, implementation, operations and maintenance, and ends with disposition of the system.

## Conclusion

The conditions noted above existed because CPD did not require its contractor to provide updated documentation in a timely manner and did not review the documentation submitted for accuracy, thereby accepting inaccurate system documentation. Should a change in contractors be made, HUD would be left with inaccurate/limited documentation to provide an incoming contractor. CPD's initiation of major modifications to the DRGR application and failure to follow HUD policy regarding the submission of documentation for the certification and accreditation process resulted in DRGR's operating under an outdated security certification for seven months. Further, CPD initiated the authorization process without the updated documentation; therefore, any results would also be based upon inaccurate information. CPD had limited assurance that the $3.9 billion in funds for NSP I and the $2 billion in funds for NSP II were not vulnerable to the security risks it is accepting, by operating without accurate documentation and proper testing.

## Recommendations

We recommend that the Office of Community Planning and Development

2A. Work with its contractors to update configuration management and contingency plans.

2B. Work with its contractors to create system and user manuals for the application.

2C. Initiate testing of the application contingency plan, once updated, and procedures to ensure that annual testing is completed.

2D. Review and revise the risk assessment to include only controls that are active and in place.

2E. Review and revise all system documentation to ensure that the information is accurate and that only valid information are maintained within the document.

2F. Submit the revised documentation to the authorizing official for use in the certification and accreditation process.

# RESULTS OF AUDIT

## Finding 3: CPD Did Not Adequately Separate the DRGR System and Security Administration Functions

CPD did not adequately separate the functions of system and security administration. This condition occurred because CPD assigned inappropriate duties to the same individual and did not establish an adequate help desk function. This error resulted in the CPD Deputy Director of Disaster Recovery being granted the authority to modify and enter grantee data and assigned the duties of security administrator. The ability to modify grantee data violated the concept of least privilege[14] and left HUD vulnerable to unauthorized data modifications.

### Separation of Duties Controls in DRGR Were Bypassed

There was no separation of duties between the DRGR system and security administrator functions. The CPD Deputy Director of Disaster Recovery performed system administration functions within DRGR. He was able to modify performance measures, add a grant, associate a grant with a grantee, and modify grantee data and was intimately involved with the development of system reports. The CPD Deputy Director of Disaster Recovery was also assigned the duties of security administrator. He was able to create user accounts and assign a user to a grantee or grant. In addition, the help desk functionality for the DRGR was inappropriately assigned to the CPD Deputy Director of Disaster Recovery and his staff. In this capacity, the Deputy Director and his staff answered e-mail requests for guidance, assistance, or data correction within DRGR. DRGR was designed with built-in controls to prohibit a user from being assigned both grantee and HUD user access. The application requires that a user be designated as a grantee or HUD user type. However, CPD bypassed this control by authorizing the creation of a HUD user profile that allowed access to modify grantee data and assigning it to the Deputy Director of Disaster Recovery and his staff. These conditions occurred because CPD inappropriately assigned system administration and security functions to the same individual and did not allocate funding for the help desk functionality services within its contract.

[14] The principle of least privilege requires that users be granted the most restrictive set of privileges (or lowest clearance) needed to perform authorized tasks (i.e., users should be able to access only the system resources needed to fulfill their job responsibilities).

U.S. Government Accountability Office's Federal Information Systems Controls Audit Manual, chapter 3, section 3.4 on segregation of duties, provides that users should be restricted from performing incompatible functions or functions beyond their responsibility. Management should analyze operations and identify incompatible duties that are then segregated through polices and organizational divisions. The manual also identifies certain functions that are generally performed by different individuals, among which are the data security (security administrator) and data administration (system administrator) functions. The data security (security administrator) function is responsible for developing security policies, procedures, and guidelines and the adequacy of access controls and service continuity procedures. The data administration (system administrator) function is responsible for planning and administering the data used throughout the entity to include installing, maintaining, and using the entity's databases and database management systems.

HUD Handbook 2400.25, REV-2, section 5.2.5, requires that program offices/system owners divide and separate duties and responsibilities of critical information system functions among different individuals to minimize the possibility that any one individual would have the necessary authority or systems access to be able to engage in fraudulent or criminal activity.

HUD Handbook 2400.25, REV-2, section 5.2.6, requires that program offices/system owners ensure that access control follows the principle of least privilege and separation of duties and that a user use unique identifiers on a system.

## Conclusion

The Deputy Director of Disaster Recovery was inappropriately assigned system and security functions for DRGR. In addition, he and his staff had inappropriate authority to modify grantee data. This level of access violated the concepts of separation of duties and least privileges. It has also resulted in an inefficient use of staff resources and may have caused unnecessary delays to users in getting assistance. It was difficult for these staff members to track user problems and the solutions. As additional grants are added to the application, the Deputy Director of Disaster Recovery and his staff may be unable to keep up with the number of requests for assistance in addition to their other official duties. The submission of grantee data is the responsibility of the grantee organization; there is no need for HUD staff to be able to modify or enter grantee data.

## Recommendations

We recommend that the Office of Community Planning and Development

3A. Separate the duties of security administration and system administration for the DRGR application.

3B. Remove the ability to modify grantee data from HUD staff members that do not require it.

3C. Take steps to fund the use of the CPD contractor to perform the help desk function for the DRGR application.

# RESULTS OF AUDIT

## Finding 4: CPD Did Not Sufficiently Test Interface Transactions between DRGR and LOCCS

CPD did not sufficiently test interface transactions[15] between DRGR and LOCCS. This condition occurred because CPD did not require the contractor to build the control tests as stated in the functional requirements document[16] and the most current system security plan (December 2008)[17]. As a result, CPD had limited assurance that the $3.9 billion in funding for NSP I and the $2 billion in funding for NSP II were accurately processed.

### CPD Did Not Sufficiently Test Interface Transactions between DRGR and LOCCS

CPD did not sufficiently test interface transactions between DRGR and LOCCS. Operational tests of errors, daily transaction totals, and out-of-balance reports of the drawdown of grant funds interface with LOCCS did not exist. However, these tests were implied as being in operation according to the functional requirements document and the most current system security plan. An independent assessment team, under the direction of the Office of the Chief Information Officer, performed security and evaluation tests of DRGR on June 10, 2009, and identified the same and other management and operational control weaknesses.

CPD did not require the contractor to build the control tests as stated in the functional requirements document and the most current system security plan. Both documents indicated that controls to perform operational tests of errors, daily transaction totals, and out-of-balance reports were used to ensure that the interface between DRGR and LOCCS operated properly. CPD staff indicated that those tests/controls were planned at one time; however, a decision was made not to

[15] Examples of interface transactions: The interface services shall be required to process drawdown requests and responses as part of the nightly voucher batch process. The system (DRGR) shall automatically submit approved voucher line items (Grantee and HQ approver if required) with a current calendar date submission date to LOCCS.

[16] The functional requirements document will contain the high-level business requirements, system requirements, and functional requirements with regard to the DRGR Release 6.3.0 system.

[17] The completion of System Security Plans is a requirement of the Office of Management and Budget Circular A-130, *Management of Federal Information Resources* and Public Law 107-347, the Federal Information Security Management Act. Federal agencies are required to identify each computer system that contains sensitive information, and to prepare and implement a plan for the security and privacy of these systems.

implement them. When that decision was made, the system documentation was not updated/corrected. Later revisions to the documentation also did not result in the removal of the inaccurate information.

NIST SP 800-53, appendix E, "Minimum Assurance Requirements," for moderate systems[18] requires that "The organization ensures that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel. . . . The organization includes documentation describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls."

HUD Handbook 2400.25, REV-2, "Information Technology Security Policy," section 3.3.5, requires that program offices/system owners ensure that adequate documentation for the information system is available, current, protected when required in compliance with NIST guidance, and distributed to authorized personnel.

HUD Handbook 2400.25, REV-2, section 3.3.5, also requires that for moderate- or high-impact systems, the documentation, if available from the vendor/manufacturer, shall describe the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

HUD Handbook 2400.25, REV-2, section 3.4.4, "Security Certification," requires program offices/system owners to follow the guidelines contained in NIST SP 800-37 and the HUD Certification and Accreditation Methodology in certifying and accrediting their information systems. Program offices/system owners shall ensure that the certification and accreditation of moderate- and high-impact systems is conducted independently. Program offices/system owners are also required to ensure that whenever changes are made to information systems; networks; or their physical environment, interfaces, or user-community makeup, the impact on the security of the information processed is reviewed via a documented security impact analysis as required by NIST SP 800-37.

**CPD Tested Interface Transactions Prior to Implementation**

The results of our limited testing of DRGR voucher data and LOCCS data and statements made by CPD indicate some testing of the interface was performed prior to implementation. We found no discrepancies in our test of paid vouchers.

[18] DRGR is defined as a 'major application' and its risk impact level is categorized as moderate.

## Conclusion

CPD used DRGR to facilitate distribution of NSP funds to grantees**.** It also used DRGR to monitor the use of NSP funds. CPD had limited assurance that the $3.9 billion in funding for NSP I and the $2 billion in funding for NSP II were accurately processed. Periodic processing and transaction tests and out-of-balance reports are controls that should be implemented to ensure accurate distribution and reporting of expenditures by grantees for NSP funds.

## Recommendations

We recommend that the Office of Community Planning and Development

4A. Work with its contractors to ensure that computer processes, both internal and external to the system, are documented and tested in accordance with NIST SP 800-53, which is incorporated in HUD policy (HUD Handbook 2400.25, REV-2).

4B. Work with its contractors to ensure that tests of drawdown controls and transaction processing reports are performed as stated in the functional requirements documentation or if other controls are used, remove stated controls not in use from system documentation.

# SCOPE AND METHODOLOGY

We performed the audit from February through August 2009 at HUD headquarters in Washington, DC, and from remote locations in Detroit, Michigan, and Kansas City, Kansas.

We reviewed CPD's DRGR documentation (functional requirements, data requirements, system security plan, risk assessment, et.al.) to gain a basic understanding of the system configuration, policies and procedures, and drawdown processes. We also interviewed CPD management officials, users, and contractors to understand the DRGR processes, controls, and risks.

We interviewed CPD management officials and its contractors to follow up on issues and/or observations noted during the course of our review.

We obtained computer-processed data from DRGR's reporting software (MicroStrategy) and LOCCS for the periods January 1 through August 12, 2009, and January 1 through June 30, 2009, respectively.

Using our generalized software application, we analyzed the DRGR and LOCCS data to identify any voucher amounts that did not match and various other validity tests of the data. Additionally, we used our generalized software application to compare user IDs recorded in various audit trail fields within DRGR.

We assessed the reliability of the DRGR data by (1) performing electronic testing of required data elements, (2) reviewing existing information about the data and the system that produced the data, and (3) interviewing agency and contractor officials knowledgeable about the data. We determined that the data were sufficiently reliable for the purposes of this report.

We conducted the audit-in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

# INTERNAL CONTROLS

Internal control is an integral component of an organization's management that provides reasonable assurance that the following controls are achieved:

- Program operations,
- Relevance and reliability of information,
- Compliance with applicable laws and regulations, and
- Safeguarding of assets and resources.

Internal controls relate to management's plans, methods, and procedures used to meet its mission, goals, and objectives. They include the processes and procedures for planning, organizing, directing, and controlling program operations as well as the systems for measuring, reporting, and monitoring program performance.

## Relevant Internal Controls

We determined that the following internal controls were relevant to our audit objective:

- Access controls,
- Output, and
- Processing.

We assessed the relevant controls identified above for the DRGR application.

A significant weakness exists if management controls do not provide reasonable assurance that the process for planning, organizing, directing, and controlling program operations will meet the organization's objectives.

## Significant Weaknesses

Based on our review, we believe that the following items are significant weaknesses:

- Access control policies and procedures violated HUD policy as reported in findings 1 and 3.
- DRGR's authorization to operate was outdated as reported in finding 2.
- CPD did not sufficiently test interface transactions between DRGR and LOCCS as reported in finding 4.

# APPENDIXES

## Appendix A

## AUDITEE COMMENTS AND OIG'S EVALUATION

**Ref to OIG Evaluation** **Auditee Comments**

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, DC 20410-7000

OFFICE OF THE ASSISTANT SECRETARY
COMMUNITY PLANNING AND DEVELOPMENT

SEP 25 2009

MEMORANDUM FOR: Hanh Do, Director, Information Systems Audit Division, GAA

FROM: Nelson R. Bregon, General Deputy Assistant Secretary, D

SUBJECT: Review of Selected Controls Within the Disaster Recovery Grant Reporting System

This memorandum is in response to OIG's draft audit report of the Office of Community Planning and Development's (CPD) Disaster Recovery Grant Reporting (DRGR) System. The draft audit report identified four findings and sixteen recommendations. With regard to many of the issues cited, CPD has already initiated actions that either address or will mitigate the cited items. CPD asks that these recommendations be deleted from the final audit report.

**Finding 1:** Access Control Policies and Procedures for DRGR Violated HUD Policy. The report finds CPD did not follow HUD policy in the creation of the access control policies and procedures for DRGR. This condition occurred because CPD did not formalize the access request process. By not implementing strong access controls, HUD could not ensure that users have access to only the data that were necessary for them to complete their jobs. In addition, HUD could not be certain that only authorized users had access to the system and that users who no longer required access to the data in the system had their access removed.

The report recommends that HUD's General Deputy Assistant Secretary for Community Planning and Development (CPD) require CPD to do the following:

1A. Establish policies and procedures requiring that all access-related requests for HUD employees be processed through CHAMP.

1B. Provide a listing of all HUD employees with access to the DRGR application and their access level to Office of Chief Information Officer, Office of Information Technology Support Services, for recording in CHAMP.

1C. Establish rules of behavior for each type of DRGR user. Implement policies and procedures requiring users to complete and sign the rules of behavior form when access is granted and annually at recertification.

1D. Establish a formal process for grantee users requesting access to the application. This process should include a requirement that an official from the applicant's organization authorize the request and the type of access required.

1E. Implement a formal user recertification process for all users of the DRGR application.

**Comment 1**

**Comment 2**

**Comment 3**

**Comment 4**

**Comment 5**

CPD Response:

1A. DRGR contractors began work in December of 2008 to integrate DRGR with Microstrategy and require CHAMP requests for all HUD users. DRGR Release 6.4 implemented on July 17, 2009 requires all HUD employees requesting access to DRGR to begin using the CHAMP process. Updated instructions for HUD user accounts were posted at hud.gov as part of the release process.

1B. A listing of all HUD employees with access to the DRGR application and their access level was provided to OCIO ADP Security personnel for recording into CHAMP in advance of the July 17, 2009 release. The result of this effort generated emails from Service Desk to all authorized users of DRGR that a change request was initiated for granting access to DRGR. All new requests for DRGR accounts after July 17, 2009 are now only created after CHAMP requests have been processed by ADP.

1C. The Rules of Behavior (ROB) item was also listed on the DRGR POAM Item C08A-1. HUD will utilize standard CIO and/or CPD rules of behavior forms for DRGR. HUD is in the process of identifying resources to distribute and collect ROB for the approximately 2,200 active DRGR users.

1D. DRGR already requires grantees to submit requests to CPD field offices for verification and approval. DRGR also requires that grantee system administrators authorize each user's access to each grant. DRGR will clarify the process to include some official from the grantee organization originate the request rather than the individual grantee user requestor. All new grantees requesting access have to be approved by the DRGR System Security Administrator prior to submission to ADP Security for processing.

1E. For several years, DRGR grantee system administrators have the ability to inactivate access to any grants for their own users as needed. Starting in late 2008, DRGR system administrators also began distributing lists of DRGR users to CPD field offices to review the accuracy and validity of grantee user accounts. Based on this, DRGR HQ administrators have worked with CPD field offices and grantees to ensure that all field offices and grantees with need for access to DRGR obtain authorization for accounts. With DRGR Release 6.4 deployed in July of 2009, HUD field office DRGR users can pull their own lists of HUD users and grantee users within their field offices along with system roles (such as requesting or approving draws). Similarly, DRGR grantee users can also see lists of their users and system roles. In accordance with standards established by CIO and CPD, DRGR HQ administrators will formalize the process for HUD and grantee managers to perform a periodic review of users.

**Finding 2:** DRGR's Authorization to Operate Was Outdated and Based upon Inaccurate and Untested System Documentation. The report finds CPD did not maintain accurate system documentation and the DRGR application operated under an outdated security certification and authorization. This condition occurred because CPD did not require its contractor to provide updated documentation in a timely manner and did not review the documentation submitted for accuracy. By accepting inaccurate system documentation, the $3.9 billion in funding for NSP I and the $2 billion in funding for NSP II are vulnerable to security exposures.

The report recommends that HUD's General Deputy Assistant Secretary for CPD require CPD to do the following:

2A. Work with its contractors to update configuration management and contingency plans.

2B. Work with its contractors to create system and user manuals for the application.

2C. Initiate testing of the application contingency plan, once updated, and procedures to ensure annual testing is completed.

2D. Review and revise the risk assessment to include only controls that are active and in place.

2E. Review and revise all system documentation to ensure that the information is accurate and that only valid information is maintained within the document.

2F. Resubmit the revised documentation for use in the certification and accreditation process.

**CPD Response:**

**Comment 2**

2A. CPD and CIO have been working on updated configuration and contingency plans as part of their ongoing system development efforts. Plans have been updated as requested.

**Comment 6**

2B. DRGR contractors have established user manuals for both modules added as part of their contract. The first was for the drawdown module in Release 6.3 from January of 2009 and the second was for the reports module in Release 6.4 from July of 2009. DRGR will continue to add user guides for the system as modifications are made to the system. System and user manuals are scheduled to be updated by May 2010 as part of Work Request 2009-003a.

**Comment 7**

2C. CPD and CIO have been working on updated configuration and contingency plans as part of their ongoing system development efforts. Testing of application contingency plan to be scheduled by SDED.

**Comment 8**

2D. CPD and CIO have been working on updated configuration and contingency plans as part of their ongoing system development efforts. Update of Risk Assessment is scheduled for next release as part of Work Request 2009-003a.

**Comment 9**

2E. Functional requirements documents are design documents intended to guide development for system programmers. HUD will continue to work with contractors to ensure that official documentation for the DRGR system includes only accurate and valid information. CPD and OCIO will continue to require contractors to update functional requirements and other required system documentation as changes are made to the system. CPD and OCIO will continue to review these documents with each new set of enhancements.

**Comment 10**

2F. CPD and CIO have been working on updated configuration and contingency plans as part of their ongoing system development efforts. All revised documentation for use in the C & A process

will be resubmitted as part of the next scheduled C & A.

**Finding 3:** CPD Did Not Adequately Separate the DRGR System and Security Administration Functions CPD did not adequately separate the functions of system and security administration. This condition occurred because CPD assigned inappropriate duties to the same individual and did not establish an adequate help desk function. This error resulted in the CPD Deputy Director of Disaster Recovery being granted the authority to modify and enter grantee data and assigned the duties of security administrator. The ability to modify grantee data violated the concept of least privileges and left HUD vulnerable to unauthorized data modifications.

The report recommends that HUD's General Deputy Assistant Secretary for CPD require CPD to do the following:

3A. Separate the duties of security administration and system administration for the DRGR application.

3B. Remove the ability to modify grantee data from HUD staff that do not require it.

3C. Take steps to fund the use of the CPD contractor to perform the help desk function for the DRGR application.

**CPD Response:**

**Comment 11**

3A. Before the deployment of DRGR Release 6.4 in July of 2009, the primary security authorization was confirmation from CPD field offices familiar with grantee operations that grantee user requests are legitimate and accurate. Since the release, all new user accounts must also include completed CHAMP requests so that ADP will establish their user IDs and passwords for DRGR.

The setup of all bank routing information will continue to be performed in LOCCS/PAS by CFO staff in Ft. Worth, Texas. Each grant has only one bank account established that cannot be altered directly by CPD staff in the DRGR system. Grantees must redistribute funds to all partner agencies and subrecipients through their own financial systems. CPD will continue to ensure that DRGR maintains separation of financial duties for grantees by requires that DRGR grantee users requesting draws are different than the DRGR grantee users approving each voucher. As before, CPD will not permit any HUD staff to function as grantee users in the grantee portion of the drawdown process.

**Comment 12**

3B. CPD will continue to restrict HUD accounts that allow edits to grantee reporting data. CPD has enforced DRGR controls that will not permit any HUD superusers to alter any obligation and drawdown data under DRGR Release 6.3 deployed in January of 2009. Financial data can only be directly altered by DRGR grantee users that have been authorized by HUD field staff familiar with grantee operations. The ability to edit grantee reporting data on their behalf will remain restricted to a very small number of HUD HQ users in order to provide technical assistance for DRGR data entry problems, as needed. HUD will continue to document any such requests by email.

**Comment 2**

3C. The addition of NSP1 into DRGR caused the number of active HUD and grantee users to increase from 100 to over 2,200. HUD has already executed a work request to allow an existing

HUD training and technical assistance contractor (Lockheed Martin) to assist with the DRGR help calls related to NSP. CPD staff submitted work request language for the help desk to the contractor on April 16, 2009. The contractor submitted a statement of work on June 8, 2009 and the work request was executed July 27, 2009. CPD trained Lockheed Martin help desk staff at their offices Aug, 11, 2009 and met with developers to build out the knowledge base system needed for help desk staff to answer questions and troubleshoot DRGR issues. The main HUD HITS help desk participated in the training remotely using a web broadcast and conference call. Lockheed Martin staff began taking DRGR help calls in September of 2009.

**Finding 4:** CPD Did Not Sufficiently' Test Interface Transactions between DRGR and LOCCS

CPD did not sufficiently test interface transactions between DRGR and LOCCS. This condition occurred because CPD did not require the contractor to build the control tests as stated in the functional requirements document and the most current system security plan (December 2008). As a result, CPD had limited assurance that the $3.9 billion in funding for NSP I and the $2 billion in funding for NSP II were accurately processed.

The report recommends that HUD's General Deputy Assistant Secretary for CPD require CPD to do the following:

4A. Work with its contractors to ensure computer processes, both internal and external to the system, are documented and tested in accordance with NIST 800-53, which is incorporated by HUD policy (HUD Handbook 2400.25 REV-2).

4B. Work with its contractors to ensure that tests of drawdown controls and transaction processing reports are performed as stated in the functional requirements documentation or, if other controls are used, removed stated controls not in use from system documentation.

**CPD Response:**

**Comment 2**

4A. CPD and OCIO will work with HUD's contractor (CACI) to ensure computer processes, both internal and external to the system, are documented and tested in accordance with NIST 800-53. Testing of drawdown functions in DRGR and LOCCS was undertaken prior to Release 6.3 deployed in January of 2009 and extensive work was conducted to ensure that self-reported amounts of disbursements in DRGR and actual disbursements in LOCCS were reconciled at the grant and activity level. Testing of drawdowns and transaction processing reports between DRGR and LOCCS will be completed as modifications/changes are completed as part of future work requests/changes to the FRD.

**Comment 13**

4B. Functional requirements documents discussed during the audit are design documents intended to guide development for system programmers. HUD will continue to work with contractors to ensure that official documentation for the DRGR system includes only accurate and valid information. All required system documentation will be updated as part of Work Request 2009-003a.

If you have any questions regarding the CPD response outlined in this memorandum, please do not hesitate to contact me or Stan Gimont, Director, Office of Block Grant Assistance at 202-708-3587.

## OIG Evaluation of Auditee Comments

Comment 1 Based on emails and changes to the DRGR webpage we acknowledge that CPD has initiated actions and is making progress related to this recommendation. We changed the recommendation wording from "Establish . . ." to "Complete . . ." to reflect CPD's efforts.

Comment 2 Upon OIG receipt and assessment of evidence supporting CPD completed actions, this recommendation can be closed concurrent with the management decision

Comment 3 CPD identified this weakness and is in the process of taking action.

Comment 4 CPD acknowledges a formal process is needed and is initiating actions to clarify and revise the current procedures.

Comment 5 CPD acknowledges that a formal process is needed and is initiating actions to clarify and revise the current procedures.

Comment 6 CPD acknowledges the weakness. However, CPD's response/proposed actions only address modifications to the system. System and user manuals should address the entire system.

Comment 7 CPD acknowledges the weakness. CPD initiated actions related to testing and acknowledges testing will be performed at a future date.

Comment 8 CPD acknowledges the weakness. CPD initiated actions related to risk assessment and acknowledges updating the risk assessment will be completed at a future date.

Comment 9 CPD acknowledges system documentation should include only accurate and valid information. OIG disagrees with CPD's statement that the functional requirements document is merely a 'design' document used by system developers. The functional requirements document defines the specific requirements for a version/release of the application. It defines the application prior to the modification and the application following the modification. It is an official record of the application used for information gathering and troubleshooting. It also provides a reader with a baseline understanding of the application, its capabilities, controls, constraints etc.

Comment 10 CPD's comments do not address the failure to provide accurate information within the recently initiated/completed C&A process. CPD should make the needed modifications to the system document and then resubmit the documentation for C&A processing. CPD should not wait until the next scheduled C&A processing.

Comment 11 CPD's comments do not address the inappropriateness of not adequately separating the functions of system and security administration. The additional information provided by CPD does not relate to the weaknesses cited.

Comment 12 No HUD staff should have the ability to modify grantee data.

Comment 13 CPD acknowledges system documentation should include only accurate and valid information. OIG disagrees with CPD's statement that the functional requirements document is merely a 'design' document used by system developers. The functional requirements document defines the specific requirements for a version/release of the application. It defines the application prior to the modification and the application following the modification. It is an official record of the application used for information gathering and troubleshooting. It also provides a reader with a baseline understanding of the application, its capabilities, controls, constraints etc.